Lecture 12.

Cyclic Codes.

__Def.__ A code $C \subset F^n$ is __cyclic__ if it is invariant under the cyclic permutation, i.e.

$(a_0 a_1 \cdots a_{n-1}) \in C \Rightarrow (a_{n-1} a_0 a_1 \cdots a_{n-2}) \in C$.

Group Algebras.

Let G be a group and let F be a field. The group algebra $F[G]$ is the set of formal linear combinations $\alpha_1 g_1 + \cdots + \alpha_n g_n$, where $\alpha_i \in F$; $g_1, \ldots, g_n \in G$ are distinct elements.

$$\left(\sum_i \alpha_i g_i\right)\left(\sum \beta_j g_j'\right) = \sum_{i,j} \alpha_i \beta_j \, g_i \cdot g_j'$$

The group algebra $F[G]$ is a ring and simultaneously it is a vector space over F.

And the "connecting" axiom holds:

$$(\alpha a) \cdot b = a \cdot (\alpha b) = \alpha (a \cdot b).$$

Such rings & vector spaces are called __algebras__.

The basis of the vector space $F[G]$ consists of group elements $g = 1 \cdot g$, $g \in G$.

Let G be the cyclic group of order n, $G = \{e, g, g^2, \dots, g^{n-1}\}$. The n-dimensional vector space F^n can be identified with $F[G]$,

$$(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \longleftrightarrow \alpha_0 \cdot e + \alpha_1 g + \dots + \alpha_{n-1} g^{n-1}$$

Let $C \subset F^n$ be a linear code. Then C can be identified with a subspace in $F[G]$, $C \subseteq F[G]$. We have

$$g(\alpha_0 e + \alpha_1 g + \dots + \alpha_{n-1} g^{n-1}) = \alpha_0 g + \alpha_1 g^2 + \dots$$

$$\dots + \alpha_{n-2} g^{n-1} + \alpha_{n-1} g^n = \alpha_{n-1} e + \alpha_0 g + \alpha_1 g^2 + \dots + \alpha_{n-2} g^{n-1}$$

Hence the code $C \subseteq F[G]$ is cyclic if and only if $gC \subseteq C$.

If $gC \subseteq C$ then $g^i C \subseteq C$ $\forall i$.

Hence $F[G]C \subseteq C$. In other words C is an ideal of the algebra $F[G]$.

We showed that

Linear cyclic codes in $F^n \overset{1-1}{\longleftrightarrow}$ ideals in $F[G]$, where G is a cyclic group of order n.

Now let us work a bit with the group algebra $F[G] = Fe + Fg + \dots + Fg^{n-1}$.

Consider the polynomial algebra $F[t]$ in one variable t and consider the mapping

$$F[t] \xrightarrow{\varphi} F[G]$$

$f(t) \xrightarrow{\varphi} f(g)$, so $\alpha_0 \cdot 1 + \alpha_1 t + \dots + \alpha_N t^N \to$ $\alpha_0 \cdot e + \alpha_1 g + \alpha_2 g^2 + \dots + \alpha_N g^N$.

This is a homomorphism of rings. It is also a linear transformation of vector spaces. Hence it is a homomorphism of algebras.

What is the $\ker\varphi$? We notice that

$$t^n - 1 \xrightarrow{\varphi} g^n - e = 0.$$

Hence $t^n - 1 \in \ker\varphi$. The ideal $(t^n-1) = (t^n-1)F[t]$ lies in $\ker\varphi$.

Consider the factor-algebra $F[t]/(t^n-1)$.

<u>Lemma</u>. An arbitrary polynomial $f(t)$ can be uniquely represented as

$$f(t) = \alpha_0 \cdot 1 + \alpha_1 t + \dots + \alpha_{n-1} t^{n-1} + (t^n-1)\, g(t).$$

<u>Proof</u>. Divide the polynomial $f(t)$ by t^n-1 with a remainder

$$f(t) = (t^n-1)g(t) + r(t), \ \deg r(t) \le n-1,$$

hence $r(t) = \alpha_0 \cdot 1 + \alpha_1 t + \dots + \alpha_{n-1} t^{n-1}$.

Uniqueness. Suppose that

$$\alpha_0 \cdot 1 + \alpha_1 t + \cdots + \alpha_{n-1} t^{n-1} + (t^n - 1) g(t) = \beta_0 \cdot 1 + \beta_1 t + \cdots + \beta_{n-1} t^{n-1}$$
$$+ (t^n - 1) h(t).$$

The polynomial $(\alpha_0 \cdot 1 + \alpha_1 t + \cdots + \alpha_{n-1} t^{n-1}) - (\beta_0 \cdot 1 + \beta_1 t + \cdots + \beta_{n-1} t^{n-1})$ has degree $\leq n-1$. At the same time this polynomial is equal to $(t^n - 1)(h(t) - g(t))$, hence divisible by $t^n - 1$. This is possible only if $\alpha_0 = \beta_0, \ldots, \alpha_{n-1} = \beta_{n-1}$.

Lemma. $\operatorname{Ker} \varphi = (t^n - 1)$.

Proof. Suppose that $f(t) \in \operatorname{Ker} \varphi$. By the previous lemma $f(t) = \alpha_0 \cdot 1 + \alpha_1 t + \cdots + \alpha_{n-1} t^{n-1} + (t^n - 1) \cancel{g(t)}\, h(t)$. We have

$$\varphi(f(t)) = \alpha_0 \cdot e + \alpha_1 g + \cdots + \alpha_{n-1} g^{n-1} = 0.$$

Since elements $e, g, \dots, g^{n-1}$ are linearly independent in $F[G]$ we conclude that $\alpha_0 = \dots = \alpha_{n-1} = 0$, $f(t) = (t^n - 1)h(t) \in (t^n - 1)$. I

By the Theorem about homomorphisms

$$F[G] \cong F[t]/(t^n - 1)$$

This implies that every cyclic linear code C can be identified with an ideal of $F[t]/(t^n-1)$.

What are ideals of $F[t]/(t^n-1)$?

For every algebra (ring) R and every ideal $I \triangleleft R$ the ideals of R/I are in 1-1 correspondence with intermediate ideals $J \triangleleft R$, $I \subseteq J \subseteq R$, $\cancel{\boxed{I = J}}$

Earlier in this course we showed

that every ideal of $F[t]$ is of the type

$(g(t)) = g(t)\,F[t]$.

Let $\quad (t^n - 1) \subseteq (g(t)) \subseteq F[t]$.

This inclusion means that $g(t)$ divides

$t^{n} - 1$, so

Linear cyclic codes in $F^n \xleftrightarrow{1-1}$ intermediate

ideals $\xleftrightarrow{1-1}$ divisors of $t^n - 1$.

We call the polynomial $g(t)$ the <u>generator</u>

<u>polynomial</u> of the code C.

To be able to say that the generator

polynomial $g(t)$ is uniquely determined

by the ideal J we demand that its leading

coefficient is equal to 1.

Let $g(t)$ be a divisor of t^n-1, $\deg g(t)=l$.

Let $t^n-1 = g(t)\,h(t)$. The polynomial $h(t)$ is called the <u>check polynomial</u> of the code C.

<u>Lemma</u>. A coset $f(t)+(t^n-1)$ lies in C if and only if $f(t)\,h(t) \in (t^n-1)$.

<u>Proof</u>. If $f(t) \in \big(g(t)\big)$ then $f(t)=g(t)\,u(t)$. Then $f(t)\,h(t) = g(t)\,h(t)\,u(t) = (t^n-1)\,u(t)$. If $f(t)\,h(t) \in (t^n-1)$ then $f(t)\,h(t) = (t^n-1)\,v(t) = g(t)\,h(t)\,v(t)$. Cancelling $h(t)$ we get $f(t) = g(t)\,v(t) \in (g(t))$. $\top$

<u>Question</u>: what is the dimension of the linear cyclic code that corresponds to a

divisor $g(t)$ of t^n-1?

In other words, what is the dimension of $C = g(t)F[t] / (t^n-1)F[t]$?

The degree of the check polynomial $h(t)$ is $n-l$.

<u>Lemma</u>. The cosets $g(t)+(t^n-1)F[t]$, $g(t)t+(t^n-1)F[t], \dots, g(t)t^{n-l-1}+(t^n-1)F[t]$ form a basis of $g(t)F[t]/(t^n-1)F[t]$.

<u>Proof</u>. <u>Linear independence</u>. Let

$$\alpha_0\big(g(t)+(t^n-1)F[t]\big)+\dots+\alpha_{n-l-1}\big(g(t)t^{n-l-1}+(t^n-1)F[t]\big)$$

$= 0$

in $g(t)F[t]/(t^n-1)F[t]$. Then

$$(\alpha_0+\alpha_1 t+\dots+\alpha_{n-l-1}t^{n-l-1})\,g(t)\in(t^n-1)F[t].$$

The degree of the left hand side is $< n$.

This is possible only if the left hand side is equal to 0, that is $\alpha_0 = \alpha_1 = \dots = \alpha_{n-\ell-1} = 0$.

<u>Span.</u> Consider an arbitrary element $a \in g(t)F[t]/(t^n-1)F[t]$, $a = g(t)f(t) + (t^n-1)F[t]$. Let us divide $f(t)$ by $h(t)$ with a remainder:

$$f(t) = \mu(t)h(t) + r(t), \ \deg r(t) < n-\ell,$$

which means that $r(t) = \alpha_0 + \alpha_1 t + \dots + \alpha_{n-\ell-1} t^{n-\ell-1}$.

Now,

$$a = \mu(t)g(t)h(t) + \sum_{i=0}^{n-\ell-1} \alpha_i\, g(t)t^i + (t^n-1)F[t],$$

which proves that the elements $g(t)t^i + (t^n-1)F[t]$, $0 \le i \le n-\ell-1$, span $g(t)F[t]/(t^n-1)F[t]$. $\top$

Corollary. $\dim_F C = n-l = \deg h(t)$.

The vector space F^n is identified with $F[t]/(t^n-1)F[t]$. Consider the basis $e_0, e_1, \dots, e_{n-1}$, $e_i = t^i + (t^n-1)F[t]$, $0 \le i \le n-1$, of this space.

Let $g(t) = \alpha_0 + \alpha_1 t + \dots + \alpha_l t^l$. In the basis $e_0, e_1, \dots, e_{n-1}$ the element $g(t) + (t^n-1)F[t]$ corresponds to the row

$$(\alpha_0, \alpha_1, \dots, \alpha_l, \underbrace{0, 0, \dots, 0}_{n-l-1})$$

The next element of the basis $g(t)t + (t^n-1)F[t]$ corresponds to the row

$$(0, \alpha_0, \alpha_1, \dots, \alpha_l, \underbrace{0, 0 \dots 0}_{n-l-2})$$, and so on.

Finally, the last basic element of the code corresponds to the row

$$(\underbrace{0\,0\cdots 0}_{n-e-1}\,\alpha_0\,\alpha_1\cdots\alpha_e)$$

Hence the <u>generator matrix</u> of C is the cyclic matrix

$$G = \left.\begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \cdots & \alpha_e & 0 & \cdots & 0 \\ 0 & \alpha_0 & \alpha_1 & \cdots & & \alpha_e & & \\ & & & \cdots & & & & \\ 0 & \cdots & 0 & \alpha_0 & \alpha_1 & \cdots & & \alpha_e \end{pmatrix}\right\} n-e$$

Let $h(t) = \beta_0 + \beta_1 t + \cdots + \beta_{n-e} t^{n-e}$. Our aim now is to find the parity check matrix H of the code C. The matrix H is a $\underbrace{\left.\begin{pmatrix} \quad & \quad \end{pmatrix}\right\}e}_{n}$ matrix with linearly independent rows such that

$$H\,G^T = 0.$$

We have

$$G^T = \underbrace{\begin{pmatrix} \alpha_0 & 0 & 0 \\ \alpha_1 & \alpha_0 & 0 \\ \vdots & & \vdots \\ \alpha_e & \vdots & \alpha_0 \\ 0 & \alpha_e & \vdots \\ 0 & 0 & \\ 0 & 0 & \alpha_e \end{pmatrix}}_{n-e} \Big\}\, n. \quad \text{If } H = \begin{pmatrix} h_1 \cdots h_n \\ \cdots \end{pmatrix}$$

then $\cancel{\alpha_0\alpha_1}\ (h_1 \cdots h_n)\cdot(\alpha_0\ \alpha_1 \cdots \alpha_e\ 0 \cdots 0) =$

$$= (\alpha_0\,\alpha_1 \cdots \alpha_e\ 0 \cdots 0)\cdot(h_1 \cdots h_n) = 0,$$

$$(h_1 \cdots h_n)\cdot(\cancel{0}\ \alpha_0\,\alpha_1 \cdots \alpha_e\ 0 \cdots 0) =$$

$$(0\ \alpha_0\,\alpha_1 \cdots \alpha_e\ 0 \cdots 0)\cdot(h_1 \cdots h_n) = 0,$$

$$\cdots$$

$$(h_1 \cdots h_n)\cdot(0 \cdots 0\ \alpha_0\,\alpha_1 \cdots \alpha_e) = (0 \cdots 0\ \alpha_0\,\alpha_1 \cdots \alpha_e)\cdot(h_1 \cdots h_n)$$

$= 0.$

<u>Trick.</u>

Suppose that we want to find the inner product

$$(x_0, x_1, \dots, x_{n-1})\cdot(y_0, y_1, \dots, y_{n-1}).$$

Consider the polynomial

$$x(t) = x_0 + x_1 t + \dots + x_{n-1} t^{n-1}$$

and the polynomial

$$y(t) = y_{n-1} + y_{n-2} t + y_{n-3} t^2 + \dots + y_0 t^{n-1}$$

(in the reverse order!).

Then the coefficient at t^{n-1} of the polynomial $x(t) \cdot y(t)$ is:

$$x_0 \cdot y_0 + x_1 \cdot y_1 + \dots + x_{n-1} y_{n-1}.$$

Let $(h_1 h_2 \dots h_n) = (0 \dots 0 \, \beta_{n-e} \, \beta_{n-e-1} \dots \beta_0)$.

Using the trick above

$$(\alpha_0 + \alpha_1 t + \dots + \alpha_e t^e + 0 \cdot t^{e+1} + \dots + 0 \cdot t^{n-1}) \cdot (\beta_0 + \beta_1 t +$$

$$\dots + \beta_{n-e} t^{n-e} + 0 \cdot t^{n-e+1} + \dots + 0 \cdot t^n) = g(t) \cdot h(t)$$

$= t^n - 1$. The coefficient at t^{n-1} is 0.

Hence

$$(\alpha_0\,\alpha_1 \cdots \alpha_\ell\; 0 \cdots 0)\cdot(0 \cdots 0\; \beta_{n-\ell}\,\beta_{n-\ell-1} \cdots \beta_0) = 0.$$

What happens if we shift $\alpha_0\,\alpha_1 \cdots \alpha_\ell$ to the right by i steps, $i \leq n-\ell-1$, and shift $\beta_{n-\ell}\,\beta_{n-\ell-1} \cdots \beta_0$ to the left by j steps, $j \leq \ell-1$, ?

In other words,

$$(\underbrace{0 \cdots 0}_{i}\; \alpha_0\,\alpha_1 \cdots \alpha_\ell\; 0 \cdots 0)\cdot(0 \cdots 0\; \beta_{n-\ell}\,\beta_{n-\ell-1} \cdots \beta_0\; \underbrace{0 \cdots 0}_{j}) \overset{?}{=} 0$$

We have

$$t^i\, g(t)\cdot t^j\, h(t) = t^{i+j}(t^n - 1),\ 0 \leq i+j \leq n-2,$$

the coefficient at t^{n-1} is zero. Hence all n-tuples $(0 \cdots 0\; \beta_{n-\ell}\,\beta_{n-\ell-1} \cdots \beta_0\; 0 \cdots 0)$ are orthogonal to all n-tuples $(0 \cdots 0\, \alpha_0\,\alpha_1 \cdots \alpha_\ell\; 0 \cdots 0)$.

This implies that the parity check matrix is

$$H = \underbrace{\begin{pmatrix} 0 \cdots 0 \ \beta_{n-\ell} \cdots \beta_0 \\ 0 \cdots \beta_{n-\ell} \ \beta_{n-\ell-1} \cdots \beta_0 \ 0 \\ \\ \beta_{n-\ell} \ \beta_{n-\ell-1} \cdots \beta_0 \ 0 \cdots 0 \end{pmatrix}}_{n} \Big\} \ell$$

<u>Example</u>. Let $n = 7$, $g(t) = x^3 + x + 1$. This is a $[7,4]$-code.

$x^7 - 1 = (x^3+x+1)(x^4+x^2+x+1)$. Hence

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

This is the Hamming code, $d = 3$, it corrects single errors.

<u>The way of encoding.</u>

It encodes 4-tuples $\leftrightarrow$ polynomials of degree 3.

$(a_0\, a_1\, a_2\, a_3) \longleftrightarrow a_0 + a_1 t + a_2 t^2 + a_3 t^3$ is encoded as $(a_0 + a_1 t + a_2 t^2 + a_3 t^3)(x^3 + x + 1) \in C$.

<u>Example</u>. $t^{23} - 1 = (t-1)(t^{11} + t^9 + t^7 + t^6 + t^5 + t + 1)(t^{11} + t^{10} + t^6 + t^5 + t^4 + t^2 + 1) =$

$= (t-1)\, g_1(t)\, g_2(t)$.

Take any of $g_1(t), g_2(t)$. The dimension is $23 - 11 = 12$. These codes are (permutation) equivalent to the binary Golay code $[23, 12, 7]$.